METHOD FOR PROTECTING COMPUTER CONNECTED TO COMPUTER NETWORK, AND RECORDING MEDIUM HAVING RECORDED PROGRAM THEREFOR

Patent Number: JP11224190
Publication date: 1999-08-17
Inventor(s): KASHIWAGI YOSHITAKA
Applicant(s):: YASKAWA ELECTRIC CORP
Requested Patent: ☐ JP11224190
Application Number: JP19980027308 19980209
Priority Number(s):
IPC Classification: G06F9/06 ; G06F15/00
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To surely protect the resources of a computer from a message with an evil intention such as a virus, etc., when a message transmitted through a computer network such as an internet, etc., is received.
SOLUTION: Before the message of an electronic mail transmitted through the internet 1 is received and read, it is checked whether a message including the instruction for an operation to destroy the resources of the computer exists or not by a filter program 4 and the message is screened and excluded at the time of existence. A processing for reading the contents of the message is executed by a message reader 3 after the filter processing of the reception message by the filter program 4.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－224190

(43)公開日　平成11年(1999)８月17日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｚ
	15/00	３１０		15/00	３１０Ｚ

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）

(21)出願番号　特願平10－27308

(22)出願日　平成10年(1998)２月９日

(71)出願人　000006622
株式会社安川電機
福岡県北九州市八幡西区黒崎城石２番１号

(72)発明者　柏木　喜孝
福岡県北九州市八幡西区黒崎城石２番１号
株式会社安川電機内

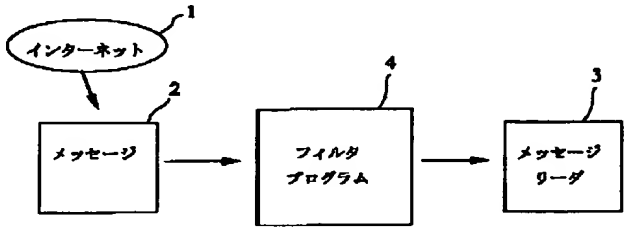
(74)代理人　弁理士　萩野　平　(外４名)

(54)【発明の名称】　コンピュータネットワーク網に接続した計算機の保護方法及びそのプログラムを記録した記録媒体

(57)【要約】

【課題】　インターネット等のコンピュータネットワーク網を介して送られてくるメッセージを受け取る場合に、ウィルス等の悪意を持ったメッセージから計算機のリソースを確実に保護する。

【解決手段】　インターネット１を介して送られてきた電子メールのメッセージ２を、メッセージリーダ３で受け取って読む前に、フィルタプログラム４によって計算機のリソースを破壊するような操作の命令を含むメッセージがないかチェックし、ある場合はそのメッセージをふるいにかけて排除する。このようなフィルタプログラム４による受信メッセージのフィルタ処理の後、メッセージリーダ３によってメッセージの内容を読む処理を行う。



1

【特許請求の範囲】

【請求項１】　コンピュータネットワーク網に接続した計算機において、このコンピュータネットワーク網を介して送られてきたメッセージを受け取った際、このメッセージを読む前に、

当該メッセージに計算機のリソースを操作するものがないかをチェックする手順と、

前記チェックによりメッセージに計算機のリソースを操作するものがあった場合にこのメッセージを排除する手順と、

を含むフィルタプログラムにより受信メッセージのフィルタ処理を行うことを特徴とするコンピュータネットワーク網に接続した計算機の保護方法。

【請求項２】　前記計算機のリソースを操作するメッセージを排除する手順として、当該メッセージを別の場所に隔離して保存することを特徴とする請求項１に記載のコンピュータネットワーク網に接続した計算機の保護方法。

【請求項３】　コンピュータネットワーク網に接続した計算機において、このコンピュータネットワーク網を介して送られてきたメッセージを受け取った際、このメッセージを読む前に、

当該メッセージに計算機のリソースを操作するものがないかをチェックする手順と、

前記チェックによりメッセージに計算機のリソースを操作するものがあった場合にこのメッセージを排除する手順と、

を含む受信メッセージのフィルタ処理を行う計算機の保護プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネットに代表されるコンピュータネットワーク網に接続した計算機の保護方法、より詳しくは、コンピュータネットワーク網を介して送られてくるメッセージに対する計算機のリソースの保護方法及びそのプログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】近年、世界的なコンピュータネットワーク網であるインターネットが広く普及しつつある。インターネットは、各地に設けられたコンピュータネットワーク同士を広域回線を介して接続したコンピュータネットワーク網であり、全世界に張り巡らされている。このインターネットを用いて電子メール等の様々なサービスが行われ、種々のメッセージがやり取りされている。インターネットメッセージの一例として電子メールを例にとり、従来用いられていた構造を図４に示す。電子メール５０は、ヘッダ５１と本文５２とからなっており、この電子メール５０にプログラム等を添付してもメッセージを読む時にはそのプログラムを実行することはできな

2

かった。そこで、MIME（MultipurposeInternet Mail Extensions ）と呼ばれる形式の電子メールが提案され、現在広く用いられている。図５にMIME形式の電子メールの構造を示す。MIME形式の電子メール６０は、ヘッダ６１と本文６２とからなっており、本文６２は複合構造を持つことができ、その中にテキスト６３、プログラム６４、画像データ６５などの複数のデータフォーマットのメッセージを含ませることができる。このとき、テキスト６３、プログラム６４及び画像データ６５などのメッセージは本文６２中に添付された形となり、メッセージを受け取ったときに添付されたメッセージを理解できるプログラムにそのメッセージを渡すことにより、メッセージに対応した処理を行うことができる。このような電子メール６０は、一般にメッセージリーダと呼ばれる電子メール処理プログラムにより処理されてメッセージが読み出される。本文６２内の各メッセージには、テキストを示す印６３ａ、プログラムを示す印６４ａ、画像データを示す印６５ａがそれぞれ設けられ、メッセージリーダはこれらの印により添付したメッセージの内容を知り、それを処理するのにふさわしいプログラムに処理を引き渡すようになっている。電子メール６０に添付されたプログラム６４に計算機のリソース（ハードウェア資源及びソフトウェア資源）を操作する命令があった場合には、メッセージリーダによりその電子メール６０のメッセージを読むと同時に計算機のリソースは操作される。このとき、リソースの操作としてディスクのフォーマットなどのリソースを破壊するような命令が含まれていた場合、計算機は大きな被害を受けることになる。従来では、前述したような電子メールに添付されたメッセージによる計算機のリソースの被害を防ぐために、以下のような方法がとられていた。従来の計算機のリソースの保護方法の例を図６及び図７に示す。図６に示す第１の方法は、メッセージリーダ７１にメッセージ７０中のあるパターン（所定のマクロプログラムなど）をチェックするチェックボックス７２を設ける方法であり、受け取ったメッセージ７０をメッセージリーダ７１で読む際に、チェックボックス７２によってリソースに被害が生じる可能性のあるメッセージを検出し、警告を発するようにしたものである。また、図７に示す第２の方法は、メッセージリーダ７１にチェック機能を備えていない場合に、ＯＳ（Operating System）７３の保護機能７４を利用する方法であり、受け取ったメッセージ７０をメッセージリーダ７１で読む際に、そのメッセージ７０に含まれる計算機のリソースを操作する命令に対して、ＯＳ７３上で保護機能７４によってリソースの被害を防ぐようにしたものである。

【０００３】

【発明が解決しようとする課題】しかしながら、前述したような従来の計算機の保護方法において、図６の方法では計算機のリソースを操作するメッセージ自体を検出

するのではなく、メッセージ中のあるパターンを見つけて警告を発するだけで、リソースの操作自体は許すために、実際に被害を受けてしまうおそれがあるという問題点があった。また、図7のOSの保護機能を利用する方法では、リソース中のユーザ領域は保護されず、さらに管理者の計算機の場合にはOSの保護機能は機能しないという問題点があった。

【0004】本発明は、上記事情に鑑みてなされたもので、インターネット等のコンピュータネットワーク網を介して送られてくるメッセージを受け取る場合に、ウィルス等の悪意を持ったメッセージから計算機のリソースを確実に保護することが可能な計算機の保護方法及びそのプログラムを記録した記録媒体を提供することを目的としている。

【0005】

【課題を解決するための手段】上記目的を達成するため、本発明の請求項1によるコンピュータネットワーク網に接続した計算機の保護方法は、コンピュータネットワーク網を介して送られてきたメッセージを受け取った際、このメッセージを読む前に、当該メッセージに計算機のリソースを操作するものがないかをチェックする手順と、前記チェックによりメッセージに計算機のリソースを操作するものがあった場合にこのメッセージを排除する手順と、を含むフィルタプログラムにより受信メッセージのフィルタ処理を行うことを特徴とする。また、請求項2によるコンピュータネットワーク網に接続した計算機の保護方法は、前記計算機のリソースを操作するメッセージを排除する手順として、当該メッセージを別の場所に隔離して保存することを特徴とする。本発明の請求項3による記録媒体は、コンピュータネットワーク網に接続した計算機において、このコンピュータネットワーク網を介して送られてきたメッセージを受け取った際、このメッセージを読む前に、当該メッセージに計算機のリソースを操作するものがないかをチェックする手順と、前記チェックによりメッセージに計算機のリソースを操作するものがあった場合にこのメッセージを排除する手順と、を含む受信メッセージのフィルタ処理を行う計算機の保護プログラムを記録したことを特徴とする。本発明では、コンピュータネットワーク網を介して受け取ったメッセージを読む前に、計算機のリソースを操作するものがないかをチェックし、メッセージに計算機のリソースを操作するものがあった場合にこのメッセージを排除することにより、ウィルスなどの悪意を持ったメッセージから計算機を保護することが可能となる。

【0006】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。図1は本発明の一実施形態に係る計算機のリソースの保護方法を示すブロック図である。本実施形態では、インターネットを通してMIME形式の電子メールによるメッセージを受け取る場合を例にとり、

計算機のリソースの保護方法を説明する。ここで、リソースとは、計算機のハードウェア資源やソフトウェア資源のことであり、ハードウェア資源としては計算機本体並びに周辺機器、さらにはローカルのネットワーク全体の装置を含み、ソフトウェア資源としてはOS関連のファイル、データファイル、プログラムファイルなどを含む。また、インターネットだけに限らず、同様の形式の内部で閉じたネットワークであるイントラネットなど、その他のコンピュータネットワーク網を通して送られてくるメッセージに対しても同様に適用することができる。本実施形態においては、インターネット1を介して送られてきた電子メールのメッセージ2を、メッセージリーダ3で受け取って読む前に、フィルタプログラム4によって計算機のリソースを破壊するような操作の命令を含むメッセージをふるいにかけて排除する。このようなフィルタプログラム4による受信メッセージのフィルタ処理の後、メッセージリーダ3によってメッセージの内容を読む処理を行う。なお、送付されたメッセージ2の受け取り処理はメッセージリーダ3自体で行っても良いし、フィルタプログラム4が代わりに受け取るようにしても良い。前記リソースを破壊するような操作としては、例えば、ディスクのフォーマット、ファイルの消去、及び大きなファイルの生成等がある。このような計算機が被害を被る操作の命令を含むメッセージを悪意を持って付加したものは一般にウィルスと呼ばれている。

【0007】図2に本実施形態に係るメッセージ読み出し処理を行う計算機の構成例を示す。パーソナルコンピュータ等からなるコンピュータ10は、ルータ11を介してインターネット1と接続されている。インターネット1とルータ11との間は、専用回線や公衆回線等によって接続されている。そして、コンピュータ10とルータ11との間は、例えばイーサネット等によるLAN（Local Area Network）12によって接続されている。コンピュータ10は、表示用のモニタ13を有し、各種処理を実行するCPU14、主記憶としてのメモリ15、ネットワークインタフェース16、ディスクインタフェース17、記録媒体としてのハードディスク18、ビデオインタフェース19等を内部に備えて構成されている。このような構成のコンピュータ10は、CPU14の動作によって、OSを立ち上げてこのOS上で各種プログラムの処理を実行する。処理動作中は、ハードディスク18に格納されたプログラムやデータを適宜メモリ15に読み込んで実行し、処理結果等をモニタ13に表示する。すなわち、プログラムの一種である前記メッセージリーダ3及びフィルタプログラム4は、ハードディスク18に格納されており、適宜メモリ15に読み込まれて処理動作が行われる。なお、フィルタプログラム4等はフロッピーディスク、CD－ROM、光磁気ディスクなどの可搬媒体に記録しておいても良い。インターネット1を通して送られてきた電子メールのメッセージ

２は、ルータ１１を介してコンピュータ１０へ伝送される。このメッセージ2は、ネットワークインタフェース１６を介してメモリ１５またはハードディスク１８の一時記憶領域に格納される。その後、フィルタプログラム４を用いたＣＰＵ１４の動作により、計算機のリソースに被害を及ぼすメッセージがないかどうかふるいにかけるフィルタ処理を行う。

【０００８】図3にフィルタプログラム４によるフィルタ処理の手順を示す。インターネット１を通して送られてきたメッセージ２を受け取った後、フィルタプログラム４はこのメッセージ２を取得する（ステップＳ１）。次いで、ウィルスとなる可能性のあるMIME形式のメッセージであるかどうかを、MIME形式のチェックで行う（ステップＳ２）。ここで、MIME形式のメッセージである場合は、ウィルスの可能性のあるフォーマットのチェック（ステップＳ３）に進む。一方、メッセージがMIME形式でない場合は、ウィルスとなる可能性がないため、メッセージリーダ３によるメッセージのリード（読み出し）処理（ステップＳ９）に進む。ステップＳ３では、メッセージ中のウィルスの可能性のあるフォーマットの有無をチェックする。ウィルスの可能性のあるフォーマットとしては、PostScript（Adobe Systems Inc.の商標）ファイル、ワードプロセッサソフト（Word）や表計算ソフト（Excel ）等のアプリケーションのマクロファイルなどがあり、これらはファイル操作、プログラムの実行、及びネットワークの操作が可能なものである。ここで、メッセージがウィルスの可能性のないフォーマットの場合はステップＳ９のメッセージのリード処理に進む。

【０００９】メッセージがウィルスの可能性のあるフォーマットの場合は、以降でメッセージが実行する操作をフィルタリングする。まず、メッセージ中の命令においてファイル操作があるかどうかをチェックする（ステップＳ４）。ここで、ファイル操作がない場合は、次のプログラムを実行しているかどうかのチェック（ステップＳ５）に進み、ファイル操作がある場合はメッセージにウィルスの可能性ありと判断する（ステップＳ７）。ステップＳ５では、メッセージ中の命令において外部プログラムを実行しているかどうかのチェックを行う。ここで、プログラムの実行がない場合は、次のネットワークを操作しているかどうかのチェック（ステップＳ６）に進み、プログラムの実行がある場合はステップＳ７に進んでメッセージにウィルスの可能性ありと判断する。ステップＳ６では、メッセージ中の命令においてネットワークに対して不要なパケットを送っているかどうかのチェックを行う。ここで、ネットワークの操作がない場合はステップＳ９のメッセージのリード処理に進み、ネットワークの操作がある場合はステップＳ７に進んでメッセージにウィルスの可能性ありと判断する。ステップＳ４～Ｓ６のチェックでＹＥＳとなり、ステップＳ７でウィルスの可能性ありと判断された場合、メッセージにウィルスの可能性があることをモニタ１３等に表示してユーザに知らせると共に、このメッセージは読まずに別の場所（別のディレクトリやフォルダ等の記録領域）に隔離して保存する（ステップＳ８）。その後、次のメッセージへ処理を進める（ステップＳ１０）。一方、ステップＳ２～Ｓ６でメッセージにウィルスの可能性がないと判断され、ステップＳ９のメッセージのリード処理に進んだ場合は、当該メッセージはウィルス等が含まれないフィルタ処理後のメッセージであるため、メッセージリーダ３によってその内容を読む。その後、ステップＳ１０で次のメッセージへ処理を進める。以降は新しいメッセージに対してステップＳ１からの手順を同様に行う。これにより、送られてきたメッセージ全部に対してウィルスの可能性があるメッセージをふるいにかけるフィルタ処理を行い、計算機のリソースを破壊するようなメッセージを排除する。このようにメッセージ内容のチェックを行うことにより、受信メッセージの検査に要する時間を短縮することができる。

【００１０】以上のように、本実施形態では、インターネット等を通してのメッセージを受け取った場合、受信したメッセージを読む前に、メッセージに計算機のリソースの操作を行うものが添付されてないかをチェックし、このような操作を含むメッセージを排除するようふるいを掛けるフィルタプログラムを備えることにより、計算機のリソースを破壊するようなウィルス等が添付された悪意を持ったメッセージから計算機のリソースを確実に保護することができる。さらに、前述したように受信したメッセージのチェック機能をフィルタプログラムという形で提供することにより、新しい機能の追加や変更、並びに計算機のメンテナンスを容易にすることができるという効果も有する。また、前記フィルタプログラムによりメッセージ内容のチェックを行うことにより、受信メッセージの検査に要する時間の短縮を図ることもできる。

【００１１】

【発明の効果】以上説明したように、本発明によれば、インターネット等のコンピュータネットワーク網を介して送られてくるメッセージを受け取る場合に、メッセージを読む前に、当該メッセージに計算機のリソースを操作するものがないかをチェックする手順と、メッセージに計算機のリソースを操作するものがあった場合にこのメッセージを排除する手順とを含むフィルタプログラムにより受信メッセージのフィルタ処理を行うことで、ウィルス等の悪意を持ったメッセージから計算機のリソースを確実に保護することが可能となる効果がある。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る計算機のリソースの保護方法を示すブロック図である。

【図２】本実施形態に係るメッセージ読み出し処理を行う計算機の構成例を示すブロック図である。

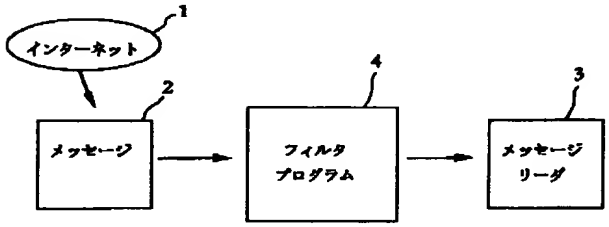
7

【図３】本実施形態のフィルタプログラムによるフィルタ処理の手順を示すフローチャートである。
【図４】従来用いられていた電子メールの構造を示す図である。
【図５】MIME形式の電子メールの構造を示す図である。
【図６】従来の計算機のリソースの保護方法の第１の例を示すブロック図である。
【図７】従来の計算機のリソースの保護方法の第２の例を示すブロック図である。
【符号の説明】
１　インターネット

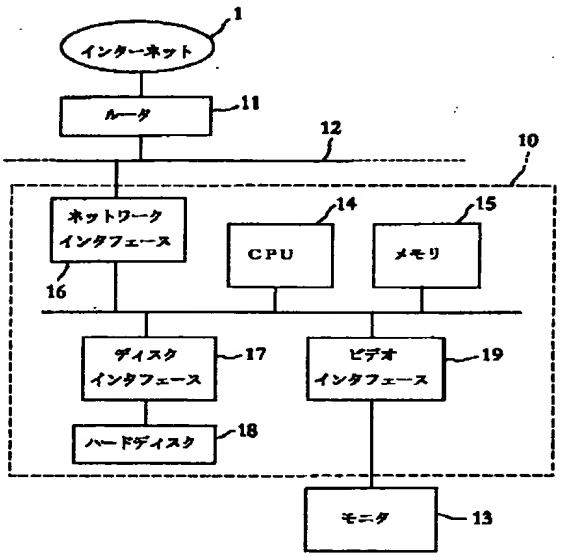
8

２　メッセージ
３　メッセージリーダ
４　フィルタプログラム
１０　コンピュータ
１１　ルータ
１２　ＬＡＮ
１４　ＣＰＵ
１５　メモリ
１６　ネットワークインタフェース
１８　ハードディスク

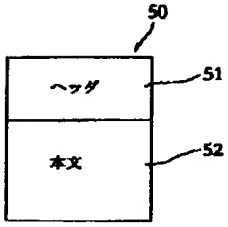
【図１】



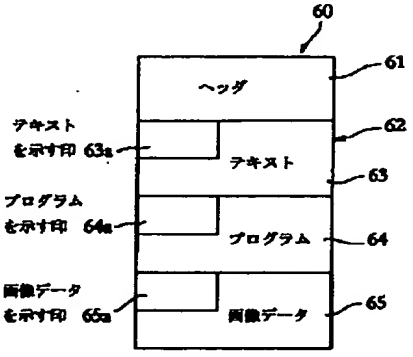
【図２】



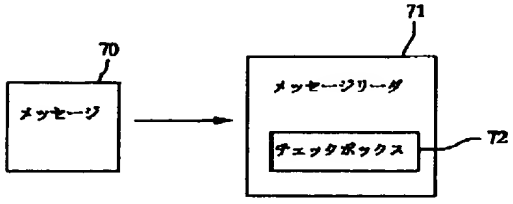
【図４】



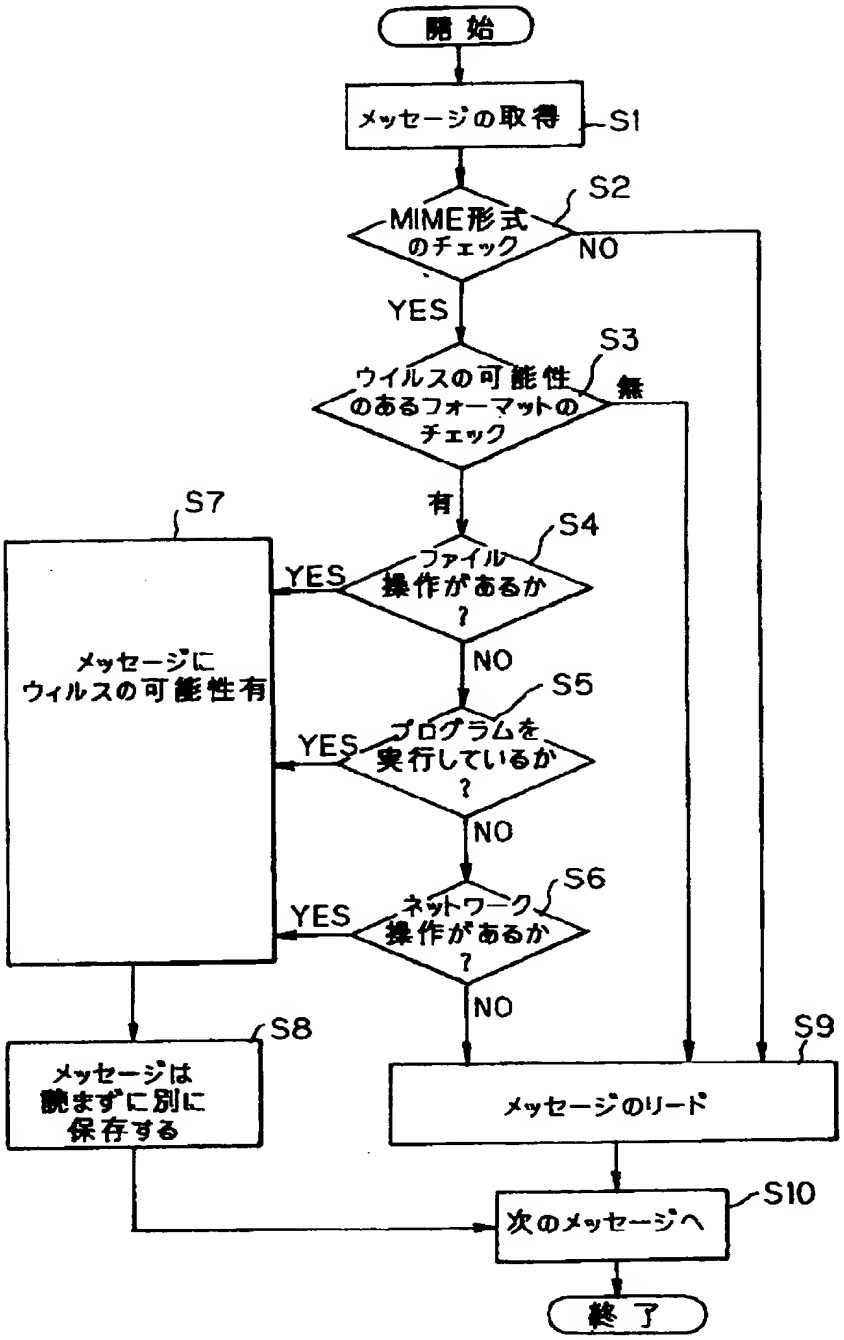
【図５】



【図６】



【図3】


開始
メッセージの取得
S1
MIME形式のチェック
S2
NO
YES
ウイルスの可能性のあるフォーマットのチェック
S3
無
有
S7
ファイル操作があるか？
S4
YES
メッセージにウィルスの可能性有
NO
プログラムを実行しているか？
S5
YES
NO
ネットワーク操作があるか？
S6
YES
NO
S8
メッセージは読まずに別に保存する
S9
メッセージのリード
次のメッセージへ
S10
終了

【図7】